



Homeland
Security

Daily Open Source Infrastructure Report

15 April 2015

Top Stories

- Russia's Ministry of Internal Affairs reported April 11 that authorities arrested the suspected developer of the Sypeng Android banking trojan along with four co-conspirators who had allegedly targeted users in the U.S. and Europe. – *Securityweek* (See item [8](#))
- The New York State Department of Financial Services released a report on cyber security in the banking sector April 9 which revealed that one in three New York banks are vulnerable to backdoors due to poor information security with third party vendors, among other findings. – *Threatpost* (See item [9](#))
- Spokane Public Schools in Washington removed 143 students from classrooms April 13 who lacked vaccination documentation or failed to file a State-mandated waiver with the district due to recent measles and whooping cough outbreaks. – *Reuters* (See item [24](#))
- Dell's annual threat report found that attacks against supervisory control and data acquisition systems (SCADA) doubled in 2014, tended to be political in nature, and targeted operational capabilities within industrial facilities. – *Securityweek* (See item [32](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *April 14, Wheeling Intelligencer/Wheeling News Register* – (West Virginia) **DEP: 132 barrels spilled into Marshall County Creek.** Two Williams Energy-owned pipelines were shut down indefinitely after heavy rains, which may have destabilized soils, triggered 132 barrels of Marcellus Shale condensate to spill into Little Grave Creek April 9. Investigators are inspecting the damage caused by the spill and the West Virginia Department of Environmental Protection reported that it planned to cite the company for several violations.
Source: <http://www.theintelligencer.net/page/content.detail/id/630514.html>

For another story, see item [32](#)

[\[Return to top\]](#)

Chemical Industry Sector

2. *April 13, KHOU 11 Houston* – (Texas) **Overtaken tanker spills hazardous chemical.** Crews worked for several hours April 13 to clear a highly flammable chemical that spilled onto the roadway from an overturned semi-truck in Channelview, Texas. About 11 residents and a nearby elementary school were ordered to shelter-in-place.
Source: <http://www.khou.com/story/news/local/2015/04/13/overtaken-tanker-spills-hazardous-chemical/25735341/>

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

3. *April 13, Chattanooga Times Free Press* – (Tennessee) **TVA starts refueling Sequoyah Unit 1.** An official at the Sequoyah Nuclear Power Plant announced April 13 that the Tennessee Valley Authority had taken the plant's Unit 1 reactor offline over the weekend of April 11 for scheduled refueling and maintenance, while the Unit 2 reactor remained online. The company will inspect components and perform equipment maintenance and upgrades during the outage.
Source: <http://www.timesfreepress.com/news/business/aroundregion/story/2015/apr/13/tva-starts-refueling-sequoyah-unit-1/298425/>
4. *April 13, Greenville Sun* – (Tennessee) **'Chemical reaction event' prompts investigation at NFS.** The U.S. Nuclear Regulatory Commission announced April 13 that it would conduct a special investigation at the Nuclear Fuel Services facility in Erwin, Tennessee, April 14 to assess the circumstances of an April 4 "unplanned chemical reaction event" involving a two-liter bottle containing cleaning materials including nitric acid and uranium stored in an access-controlled storage area. There were no reports of injury or exposure as a result of the incident.
Source: http://www.greenvillesun.com/news/local_news/chemical-reaction-event-

[prompts-investigation-at-nfs/article_a3693d9c-e232-11e4-a871-fb8bab22baf3.html](https://www.somdnews.com/article_a3693d9c-e232-11e4-a871-fb8bab22baf3.html)

5. *April 13, SoMdNews.com* – (Maryland) **Calvert Cliffs nuclear plant restored to full power.** Operators at Calvert Cliffs Nuclear Power Plant in Maryland returned the plant to full power April 10 following an automatic shutdown that occurred as a result of an offsite grid disturbance that caused widespread power outages in the region April 7. Investigators began a series of comprehensive testing prior to the synchronization of both units to the power grid.
Source: <http://www.somdnews.com/article/20150413/NEWS/150419809/calvert-cliffs-nuclear-plant-restored-to-full-power&template=southernMaryland>
6. *April 13, Associated Press* – (Nebraska) **Fort Calhoun nuclear plant shut down for refueling.** Omaha Public Power District officials reported that the Fort Calhoun Nuclear Generating Station in Blair, Nebraska, was taken offline for scheduled refueling and maintenance April 11. Employees will also perform preventive maintenance and testing, and replace equipment and instrumentation during the outage, which is expected to last 45 days.
Source: <http://www.mysanantonio.com/business/energy/article/Fort-Calhoun-nuclear-plant-shut-down-for-refueling-6196488.php>

[\[Return to top\]](#)

Critical Manufacturing Sector

See item [32](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

7. *April 14, Associated Press* – (National) **Ex-Assembly speaker's son-in-law charged in \$7M Ponzi scheme.** A New York investment manager and co-owner of Allese Capital was charged April 13 with defrauding investors out of \$7 million in a Ponzi scheme in which he allegedly solicited securities trading investments from 2009 – 2014, and only invested portions of the funds, while using the remainder for his own benefit and to repay other investors.
Source: http://www.omaha.com/news/nation/ex-assemblyman-s-son-in-law-facing-federal-fraud-charges/article_a6b21895-0b00-5df8-a07c-2d3b42cf6663.html
8. *April 14, Securityweek* – (International) **Alleged creator of Svpeng Android malware arrested in Russia.** Russia's Ministry of Internal Affairs reported April 11 that the

suspected developer of the Svpeng Android trojan along with 4 co-conspirators calling themselves “The Fascists” who had allegedly used the trojan to steal money from bank accounts in the U.S. and Europe were arrested. The malware employs a combination of short message service (SMS) hacking, phishing Web pages, credential logging, and ransomware to access victims’ account and access funds.

Source: <http://www.securityweek.com/alleged-creator-svpeng-android-malware-arrested-russia>

9. *April 13, Threatpost* – (New York) **Vulnerabilities identified in NY banking vendors.** The New York State Department of Financial Services released a report on cyber security in the banking sector April 9 which revealed that one in three New York banks are neglectful of information security relating to third-party vendors and are vulnerable to backdoor access by those looking to steal data as a result. One in three banks interviewed did not require vendors to notify them in the event of a data breach, and only half had strategies prepared for breach scenarios, among other findings.
Source: <https://threatpost.com/vulnerabilities-identified-in-ny-banking-vendors/112209>

[\[Return to top\]](#)

Transportation Systems Sector

10. *April 14, Associated Press* – (Washington) **Worker wakes from nap in cargo hold.** The Federal Aviation Administration is investigating after an Alaska Airlines flight bound for Los Angeles returned to Seattle-Tacoma International Airport for an emergency landing April 13 when the pilots heard screams for help from an airport worker who allegedly fell asleep and became trapped in the cargo hold. The employee appeared unhurt and was transported to a hospital as a precaution, while the flight continued onto its final destination.
Source: <https://www.indianagazette.com/news/reg-national-world/worker-wakes-from-nap-in-cargo-hold,21856423/>
11. *April 14, Dallas Morning News* – (Texas) **Eastbound I-20 reopens in Balch Springs after tractor-trailer crashes into sign.** Three lanes on Interstate 20 Eastbound in Balch Springs reopened and 1 remained closed for at least 10 hours while crews cleaned up a fuel spill caused when a semi-truck hydroplaned and struck a pole supporting a sign that spanned the eastbound lanes April 14. The driver of the semi-truck was taken to a local hospital with non-life-threatening injuries.
Source: <http://thescoopblog.dallasnews.com/2015/04/eastbound-i-20-shut-down-after-tractor-trailer-crashes-burns-in-balch-springs.html/>
12. *April 13, KMGH 7 Denver* – (Washington, D.C.; Colorado) **United Airlines flight from Reagan to DIA delayed for ‘security issue’, FBI investigating.** United Airlines officials reported April 13 that a flight from Washington, D.C. to Denver was delayed nearly 3 hours due to an unspecified security issue that prompted passengers to be evacuated and re-screened by TSA. The FBI searched the plane before it was cleared to depart for its final destination.
Source: <http://www.thedenverchannel.com/news/front-range/denver/united-airlines->

[flight-from-reagan-to-dia-delayed-for-security-issue-fbi-investigating](#)

For another story, see item [25](#)

[\[Return to top\]](#)

Food and Agriculture Sector

13. *April 13, Associated Press* – (Wisconsin) **Wisconsin records 1st outbreak of H5N2 bird flu strain.** Authorities confirmed April 13 the presence of the H5N2 avian flu strain in a commercial flock of about 200,000 chickens in Jefferson County, Wisconsin, and that the entire flock will be culled to prevent the disease from spreading. The disease has resulted in the death of more than 1.2 million turkeys across the Midwest, including 900,000 birds in Minnesota where turkey producers have reportedly suffered an estimated \$15.7 million in losses associated with the outbreak.
Source: <http://minnesota.cbslocal.com/2015/04/13/wisconsin-records-1st-outbreak-of-h5n2-bird-flu-strain/>
14. *April 13, U.S. Department of Agriculture* – (Pennsylvania; New York) **Leader Slaughterhouse, LLC recalls veal carcasses produced without full benefit of inspection.** The Food Safety and Inspection Service announced April 13 that Leader Slaughterhouse, LLC, recalled about 1,800 pounds of veal carcasses that were produced without the full benefit of Federal inspection and outside inspection hours. The recalled product was picked up at the company's location in Imler, Pennsylvania, and taken by customers to Pennsylvania and New York.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-060-2015-release>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

15. *April 14, WDAF 4 Kansas City* – (Missouri) **North Kansas City Hospital closes ER to ambulances, reschedules surgeries.** The North Kansas City Hospital in Missouri reported that patient care was not affected after a water main break spilled about 500,000 gallons of water onto streets and prompted the closure of its emergency room to all ambulances, and canceled morning surgeries and procedures April 14. Crews worked to repair the break and officials issued a boil order for the areas within a block of the break.
Source: <http://fox4kc.com/2015/04/14/north-kansas-city-hospital-closes-er-to-ambulances-reschedules-surgeries/>
16. *April 13, Gulf Coast News Today* – (Alabama) **Health Department issues sewage spill notice for Rock Creek in Robertsedale.** The City of Robertsedale reported April 13 that the health department urged residents to exercise caution if using Rock Creek for recreational purposes, after a lift station overflowed and discharged an estimated 10,000 – 100,000 gallons of sewage into the creek following heavy rainfall.

Source: http://www.gulfcoastnewstoday.com/area_news/article_0f84f6ce-e229-11e4-810d-d34bb3ec53c1.html

17. *April 13, Orange County Register* – (California) **Sewage spill closes portion of Newport Bay until at least Wednesday.** Nearly 750 gallons of raw sewage spilled from a manhole into Newport Bay April 13 prompting health officials to close a portion of the water area to swimming and diving until further notice pending water sample testing. Closure signs were posted along the Pacific Coast Highway and there were no reports of sickness or injury as a result of the spill.

Source: <http://www.ocregister.com/articles/morning-657821-notice-close.html>

For another story, see item [1](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

18. *April 13, Charleston Gazette* – (West Virginia) **VA clinic in Greenbrier County to close indefinitely.** Officials reported that the Veterans Affairs Greenbrier County Community-Based Outpatient Clinic in Maxwelton was closed April 13 until further notice after air quality tests in March found elevated levels of formaldehyde in the air. Medical services were temporarily relocated to the Veterans Administration Medical Center in Beckley.

Source: <http://www.wvgazette.com/article/20150413/GZ01/150419765>

For additional stories, see items [15](#) and [24](#)

[\[Return to top\]](#)

Government Facilities Sector

19. *April 14, Associated Press* – (North Carolina; Florida) **North Carolina college shooting suspect arrested in Florida.** A man suspected of fatally shooting a former boss at Wayne County Community College in North Carolina April 13, that prompted a lockdown and manhunt, was arrested without incident in Daytona Beach, Florida, April 14 after an officer found him asleep on a beach. Authorities were working to extradite the suspect to North Carolina to face charges.

Source: <http://www.sfgate.com/news/crime/article/Classes-resume-at-NC-college-where-instructor-was-6198204.php>

20. *April 14, New Orleans Times-Picayune* – (Louisiana) **Suspect in shooting of 3 Cohen Prep students bought shrimp plate then began firing, NOPD says.** New Orleans police reported April 14 that a suspect was in custody following a triple shooting at a Central City bus stop April 13 that left 3 Cohen Prep students injured. Police are investigating the incident and believe that the suspect was unprovoked when he began firing into the crowd at the bus stop.

Source:

http://www.nola.com/crime/index.ssf/2015/04/suspect_in_triple_shooting_at.html

21. *April 13, Muncie Star Press* – (Indiana) **9 students taken to hospital after Muncie bus crash.** A driver and 9 students from East Washington Academy were transported to an area hospital after a school bus collided with a vehicle traveling the wrong way in Muncie April 13.
Source: <http://www.thestarpress.com/story/news/local/2015/04/13/9-students-taken-to-hospital-after-muncie-bus-crash/25708333/>
22. *April 13, Associated Press* – (New York) **Police: Bomb threat at Hamilton College unfounded, lockdown ends.** New York State Police cleared the scene and lifted a lockdown after more than 8 hours following a search of Hamilton College after a phoned bomb threat prompted the cancelation of classes and a shelter-in-place order for students April 13.
Source: http://auburnpub.com/news/local/police-bomb-threat-at-hamilton-college-unfounded-lockdown-ends/article_91cba156-e1f6-11e4-80e4-b30c4ae163bd.html
23. *April 13, WKMG 6 Orlando* – (Florida) **Students taken to hospital in Brevard school bus crash.** Four Central Middle School students and a driver were transported to a local hospital after a school bus and vehicle collided in Palm Bay April 13.
Source: <http://www.clickorlando.com/news/students-taken-to-hospital-in-brevard-school-bus-crash/32337912>
24. *April 13, Reuters* – (Washington) **Washington state school district removes 143 students over vaccine law.** Spokane Public Schools in Washington removed 143 students from classrooms April 13 who lacked documentation confirming that they had received vaccinations or had filed a State-mandated waiver with the district due to a recent measles epidemic that affected over 150 people across the U.S., and a whooping cough outbreak in the State's eastern city.
Source: <http://www.reuters.com/article/2015/04/14/us-usa-vaccine-washington-idUSKBN0N507020150414>
25. *April 13, Helena Independent Record* – (Montana) **No threat found in suspicious package at federal building.** The Baucus Federal Building, Paul G. Hatfield Federal Courthouse, and the State of Montana mail processing facility in Helena were evacuated for several hours April 13 after a suspicious package was delivered to the main entrance of the Federal building. A bomb squad removed the package and deemed it safe after inspecting it at a disposal site.
Source: http://helenair.com/news/local/federal-buildings-in-helena-evacuated-due-to-suspicious-package/article_fa0cf346-507d-50af-bb12-8b6872949ecb.html
26. *April 13, Houston Chronicle* – (Texas) **Victim dead, students hurt after 2 separate bus crashes.** A bus driver, 1 adult, and 13 students were transported to area hospitals after 2 Houston Independent School District buses collided at the intersection of Bacher at Bonaire April 13.
Source: <http://www.chron.com/houston/article/2-HISD-school-buses-collide-in->

northeast-Houston-6197125.php

For additional stories, see items [27](#) and [32](#)

[\[Return to top\]](#)

Emergency Services Sector

27. *April 14, St. Paul Pioneer Press* – (Minnesota) **Minneapolis dispatchers evacuate during city hall fire.** Emergency 9-1-1 employees were evacuated for over 4 hours due to smoke following an April 13 fire at the Minneapolis City Hall building that began in the Minneapolis Police Department's property room, located in the building's subbasement. The property room was closed indefinitely while police evaluated the extent of damage to items within.

Source: <http://www.firehouse.com/news/11918222/minneapolis-dispatchers-evacuate-during-city-hall-fire>

For another story, see item [15](#)

[\[Return to top\]](#)

Information Technology Sector

28. *April 14, Softpedia* – (International) **Misconfigured DNS servers vulnerable to domain info leak.** The U.S. Computer Emergency Readiness Team (US-CERT) released a security statement warning that misconfigured, public-facing domain name system (DNS) servers utilizing Asynchronous Transfer Full Range (AXFR) protocols are vulnerable to system takeovers, redirects to spoofed addresses, and denial-of-service (DoS) attacks from unauthenticated users via DNS zone transfer requests. Research from Alexa revealed that over 72,000 domains and 48,000 nameservers were affected by the issue.

Source: <http://news.softpedia.com/news/Misconfigured-DNS-Servers-Vulnerable-to-Domain-Info-Leak-478331.shtml>

29. *April 14, Help Net Security* – (International) **18-year-old bug can be exploited to steal credentials of Windows users.** A Cylance researcher identified a new technique for exploiting an 18-year-old flaw in Windows Server Message Block (SMB) in all versions of Windows operating systems (OS) which allows attackers to intercept user credentials by hijacking communications with legitimate Web servers via man-in-the-middle (MitM) attacks that send them to malicious server message block (SMB) servers that reveal victims' usernames, domains, and hashed passwords.

Source: <http://www.net-security.org/secworld.php?id=18210>

30. *April 14, Help Net Security* – (International) **Attackers use deceptive tactics to dominate corporate networks.** Symantec released research revealing that spear-phishing attacks on corporations increased by 8 percent in 2014, and that email and social media had remained significant attack vectors. Researchers also found that

software companies took an average of 59 days to release patches and that 24 zero-day vulnerabilities were discovered in 2014, among other findings.

Source: <http://www.net-security.org/secworld.php?id=18208>

31. *April 13, Help Net Security* – (International) **Attackers can easily crack Belkin routers' WPS PINs.** A security researcher discovered that 80 percent of Belkin routers tested generated Wi-Fi Protected Setup (WPS) PINs based on the device's own MAC addresses and serial numbers, leaving it vulnerable to discovery by attackers using unencrypted request/response packets via Wi-Fi probes.

Source: <http://www.net-security.org/secworld.php?id=18204>

32. *April 13, Securityweek* – (International) **Attacks against SCADA systems doubled in 2014: Dell.** Dell revealed in its annual threat report that attacks against supervisory control and data acquisition systems (SCADA) doubled in 2014, including 51,258 attacks in the U.S., and that the attacks tended to be political in nature and targeted operational capabilities within power plants, factories, and refineries primarily in Finland, the U.K., and the U.S. The report found that 25 percent of the attacks witnessed exploited buffer overflow vulnerabilities followed by improper input validation and information exposure.

Source: <http://www.securityweek.com/attacks-against-scada-systems-doubled-2014-dell>

For additional stories, see items [8](#) and [9](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

Nothing to report

[\[Return to top\]](#)

Commercial Facilities Sector

33. *April 14, WABC 7 New York City; Associated Press* – (New Jersey) **Firefighters investigate 5-alarm fire that gutted South Amboy C-Town.** A 5-alarm fire at the C-Town Supermarket in South Amboy April 13 destroyed the grocery store that was undergoing repairs and scheduled to reopen during the week of April 20 following a January fire. The cause of the April 13 fire remains under investigation.

Source: <http://7online.com/news/4-alarm-fire-guts-south-amboy-supermarket/656361/>

34. *April 14, KTVI 2 St. Louis* – (Missouri) **Seniors, disabled residents evacuated due to Midtown apartment fire.** About 60 residents were evacuated from the Metropolitan Village Apartments in St. Louis after a fire broke out April 14. Three residents were transported to an area hospital and nine others were treated at the scene for non-life-threatening injuries.
Source: <http://fox2now.com/2015/04/14/seniors-disabled-residents-evacuated-due-to-midtown-apartment-fire/>
35. *April 14, WLBT 3 Jackson/WDBD 40 Jackson* – (Mississippi) **Fire at a Ridgeland hotel leads to evacuation.** About 65-70 guests and staff were evacuated from the Extended Stay Hotel in Ridgeland and relocated to different hotels April 13 after a grease fire activated the building's sprinkler system. Crews worked through April 14 to inspect electrical systems and the sprinkler system, and to clean up water and fire damage throughout the building.
Source: <http://www.wdam.com/story/28793510/fire-at-a-ridgeland-hotel-leads-to-evacuation>
36. *April 13, Atlanta Journal-Constitution* – (Georgia) **Gwinnett hotel temporarily evacuated after gas leak.** About 125 guests and staff were evacuated from the Hilton Atlanta Northeast hotel in Gwinnett County April 13 due to a carbon monoxide leak from an unidentified source in the building's basement boiler room. Gas service was cut off and guests were allowed to return about 5 hours later, while seven employees were evaluated at the scene for minor sickness.
Source: <http://www.ajc.com/news/news/gwinnett-hotel-evacuated-after-possible-gas-leak/nksk4/>
37. *April 13, U.S. Environmental Protection Agency* – (Idaho) **EPA: Boise-based ski and snowboard park developer required to properly clean up asbestos to protect workers and area residents.** The U.S. Environmental Protection Agency issued an asbestos abatement Compliance Order to Gateway Parks LLC, April 13 after the company initiated the partial demolition of the Lazy J Tavern complex near Eagle, Idaho, in 2014, without safely removing asbestos that was found during inspection. The order requires Gateway Parks to clean up contaminated debris from the partially-demolished buildings and to follow all relevant laws and regulations for future demolition projects on the property.
Source: <http://yosemite.epa.gov/opa/admpress.nsf/21b8983ffa5d0e4685257dd4006b85e2/5c99371d37bd98e185257e26007a25dd!OpenDocument>

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes .
Removal from Distribution List:	Send mail to support@govdelivery.com .

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.